Method for establishing a common code for authorized persons through a central office

Patent Number: US5903649
Publication date: 1999-05-11
Inventor(s): SCHWENK JOERG (DE)
Applicant(s):: DEUTSCHE TELEKOM AG (DE)
Requested Patent: DE19538385
Application Number: US19960731364 19961011
Priority Number(s): DE19951038385 19951014
IPC Classification: H04L9/00 ; H04N7/16
EC Classification: H04L9/08
Equivalents: AU6572796, AU721074, CA2181972, EP0768773, B1, NO962672, NZ299014

Abstract

To provide sufficient security, a method, based on the use of a code-controlled one-way function with a threshold scheme, is described. N shadows si are derived from the personal code of each of n authorized persons in the central office, a code k is calculated in the central office from the n shadows si, . . . sn using an (n, t) threshold scheme, and the data for establishing code k is transmitted though an unsecured channel. The data for establishing code k comprises data required for deriving shadows si from the personal codes ki and n-1 other shadows of the (n,t) threshold scheme, which other shadows differ from the shadows of the authorized persons. The method can be used for a plurality of purposes; however, it is specifically designed for providing security in the transmission of a broadcast program subject to fees (pay-TV, pay-radio).

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 38 385 A 1**

(51) Int. Cl.[6]:
H 04 L 9/32
// H04N 7/16,G07C 9/00,G06F 12/14

(21) Aktenzeichen: 195 38 385.0
(22) Anmeldetag: 14. 10. 95
(43) Offenlegungstag: 17. 4. 97

DE 195 38 385 A 1

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Schwenk, Jörg, Dr.rer.nat., 64846 Groß-Zimmern, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

US 51 99 070
US 51 24 117
Using A Local Password For Two-Step Authentication. In: IBM Technical Disclosure Bulletin, Vol.35, No.4A, Sept. 1992, S.373- S.375;
ZU-HUA,S.: Public-key cryptosystem and digital-signature schemes based on linear algebra over a local ring. In: IEE Proceedings, Vol.134, Pt.E, No.5, Sept. 1987, S.254-256;

(54) Verfahren zur Etablierung eines gemeinsamen Schlüssels für autorisierte Personen durch eine Zentrale

(57) Für die Schlüsseletablierung für autorisierte Personen werden Schlüssel k verschlüsselt übertragen, was teilweise auf rechtliche Vorbehalte stößt.
Um solchen Vorbehalten zu begegnen und gleichzeitig hinreichende Sicherheit zu bieten, wird ein Verfahren beschrieben, das auf einer Kombination einer schlüsselgesteuerten Einwegfunktion mit einem Threshold-Verfahren beruht.
Das Verfahren ist für viele Zwecke anwendbar; jedoch prädestiniert für die Sicherung der Übertragung eines gebührenpflichtigen Rundfunkprogramms (Pay-TV, Pay-Radio).

DE 195 38 385 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren der im Oberbegriff des Patentanspruchs 1 näher definierten Art. Ein derartiges Verfahren ist beispielsweise in DIN EN 50 094 für Pay-TV-System Eurocrypt aufgeführt. Es dient zum Etablieren einer gemeinsamen geheimen Information k (Schlüssel) für autorisierte Personen aus einer größeren Personengruppe $P = \{P_1, \ldots P_m\}$ durch eine zentrale Instanz Z (Zentrale).

Die Zentrale entscheidet darüber, welche Personen aus einer Personengruppe autorisiert sind. Das Verfahren garantiert, daß nur diese Personen den Schlüssel erhalten bzw. berechnen können. Die autorisierten Personen seien im folgenden o. B. d. A. mit $P_1, \ldots, P_n$ bezeichnet (so daß also $n \leq m$ gilt). Nachrichten der Zentrale an die Benutzer können über ein Rundfunkmedium (terrestrischer Rundfunk, Satellit, Kabelnetz) oder andere ungesicherte Kanäle an die Personen aus P gesendet werden.

Bekannt ist die Verwendung eines symmetrischen Verschlüsselungsalgorithmus (für die Definition eines symmetrischen Verschlüsselungsalgorithmus siehe auch A. Beutelspacher: Kryptologie, Vieweg Verlag 1994). Jeder Person P_i aus P ist ein persönlicher Schlüssel k_i zugeordnet, den nur die Person selbst und die Zentrale kennen. Die Zentrale Z wählt nur den Schlüssel k und verschlüsselt ihn für $i = 1, \ldots, N$ mit dem jeweiligen persönlichen Schlüssel k_i:

$$C_i = E(k_i, k).$$

Dieses Kryptogramm wird dann an die (autorisierte) Person P_i geschickt, die den Schlüssel k berechnen kann, indem sie das Kryptogramm entschlüsselt:

$$D(k_i, C_i) = D(k_i, E(k_i, k)) = k.$$

Dieses Verfahren wird z. B. im Pay-TV-System Eurocrypt (DIN EN 50 094) zur Etablierung eines Systemschlüssels eingesetzt.

Der Nachteil dieses Verfahrens besteht darin, daß der Schlüssel k verschlüsselt übertragen wird. In vielen Staaten steht die Verwendung eines Verschlüsselungsalgorithmus unter rechtlichen Vorbehalten. Dies könnte z. B. dazu führen, daß der oben verwendete Algorithmus E (für engl. "encryption") sehr schwach sein muß.

Der Erfindung liegt die Aufgabe zugrunde, ein allgemeiner unbedenklich anwendbares Verfahren anzugeben, das gleichzeitig hinreichend sicher ist.

Diese Aufgabe wird mit den im Kennzeichen des Patentanspruchs 1 dargelegten Verfahrensschritten gelöst.

Hinsichtlich erhöhter Sicherheit sind vorteilhafte Weiterbildungen in den Kennzeichen der Unteransprüche 2 bis 4 angeführt.

Die Erfindung, die nachfolgend an Ausführungsbeispielen näher beschrieben wird, besteht darin, mit Methoden der symmetrischen Kryptographie die Funktionalität des oben beschriebenen Verfahrens nachzubilden, ohne Verschlüsselungsverfahren zu verwenden. Dadurch kann bei Einhaltung rechtlicher Bestimmungen die Sicherheit des Schlüsselverteilmechanismus verbessert werden.

Die hier beschriebene Erfindung beruht auf einer Kombination einer schlüsselgesteuerten Einwegfunktion mit einem Threshold-Verfahren (A. Shamir: How to Share a Secret. Comm. ACM, Vol. 24, Nr. 11, 1979, 118–119).

Eine Einwegfunktion (vgl. Beutelspacher, s. o.) ist eine Funktion $g(\cdot)$, die sich leicht auswerten läßt (d. h. für jeden Wert a ist g(a) leicht berechenbar), für die es aber praktisch unmöglich ist, zu einem gegebenen Bildwert b ein Urbild a zu finden, so daß $g(a) = b$ gilt. Eine schlüsselgesteuerte Einwegfunktion ist eine Einwegfunktion $f(\cdot,\cdot)$ mit zwei Argumenten k und a, wobei der Wert k als Schlüssel angesehen werden kann.

Mit einem (n,t)-Threshold-Verfahren kann man ein Geheimnis k so in t Teile, die Shadows genannt werden, zerlegen, daß dieses Geheimnis aus je n der t Shadows rekonstruiert werden kann.

Als Beispiel für ein solches (n,t)-Threshold-Verfahren soll im folgenden ein Polynom vom Grad $n-1$ dienen, aus dem $t = 2n-1$ Stützstellen als Shadows ausgewählt werden. Durch Angabe von n Stützstellen, d. h. von n Paaren (x_i, y_i) $(i = 1, \ldots, n)$ von Elementen eines Körpers mit unterschiedlichen x-Komponenten, wird ein eindeutiges Polynom vom Grad $n-1$ definiert. Dieses Polynom schneidet die y-Achse in einem eindeutig definierten Punkt.

Zur Etablierung eines gemeinsamen Schlüssels für die autorisierten Personen $P_1, \ldots, P_n$ wird zunächst jeder Person P_j aus P unter Verwendung des persönlichen Schlüssels k_j eine Stützstelle (a_j, b_j) zugeordnet. Dies kann auf verschiedene Art und Weise geschehen:

1. $(a_j, b_j) := (j, k_j)$,

2. $(a_j, b_j) := (j, g(k_j))$ für eine Einwegfunktion $g(\cdot)$,

3. $(a_j, b_j) := (j, f(r, k_j))$ für eine schlüsselgesteuerte Einwegfunktion $f(\cdot,\cdot)$ und eine Zufallszahl r,

4. $(a_j, b_j) := (f(r, l_j), f(r, l_j'))$ für eine schlüsselgesteuerte Einwegfunktion $f(\cdot,\cdot)$, eine Zufallszahl r und $k_j = (l_j, l_j')$,

usw.

Durch die Stützstellen $(a_1, b_1), \ldots, (a_n, b_n)$ wird ein Polynom p(x) vom Grad $n-1$ festgelegt. Der eindeutige Schnittpunkt

$$k := p(0)$$

dieses Polynoms mit der y-Achse ist der gemeinsame Schlüssel für $P_1, \ldots, P_n$. Damit die autorisierten Personen $P_1, \ldots, P_n$ diesen Wert k berechnen können, wählt die Zentrale $n-1$ weitere Stützstellen $(c_1, d_1), \ldots, (c_{n-1}, d_{n-1})$, die von $(a_1, b_1), \ldots, (a_n, b_n)$ verschieden sein müssen. Diese können zusammen mit der zur Berechnung der Stützstellen nötigen Zusatzinformation (z. B. die Zufallszahl r aus 3.) an alle Personen aus P gesendet werden.

Nur die autorisierten Personen P_j $(1 \leq j \leq n)$ können jetzt den Schlüssel k berechnen. Dazu fügt P_j der Menge $(c_1, d_1), \ldots, (c_{n-1}, d_{n-1})$ die Stützstelle (a_j, b_j) hinzu, die nur er und die Zentrale berechnen können, da nur er und die Zentrale den persönlichen Schlüssel k_j kennen. Die so erhaltenen n Stützstellen legen das Polynom p(x) und damit auch die Zahl $k = p(0)$ eindeutig fest.

Die nicht autorisierten Personen P_i $(n+1 \leq j \leq m)$ können den Schlüssel k nicht berechnen, da die von ihnen berechenbaren Stützstellen (a_i, b_i) nicht auf dem Graphen von p(x) liegen.

Eine empfohlene Realisierung der hier vorgestellten Erfindung sollte zur Ableitung der Stützstellen eine schlüsselgesteuerte Einwegfunktion, also eine Variante

der Verfahren (3.) oder (4.) verwenden, um mögliche Angriffe auszuschließen, die bei Verwendung der schwächeren Varianten (1.) und (2.) möglich wären. In diesem Fall kann gezeigt werden, daß ein nicht autorisierter Angreifer einen nach diesem Verfahren etablierten Schlüssel k nur dann brechen könnte, wenn er die Einwegfunktion umkehren könnte.

Patentansprüche

1. Verfahren zur Etablierung eines gemeinsamen Schlüssels k für autorisierte Personen, wobei die Menge der autorisierten Personen eine sich zeitlich ändernde Teilmenge einer Gesamtmenge von Teilnehmern ist, durch eine Zentrale Z über ungesicherte Kanäle, insbesondere ein Rundfunkmedium, bei dem die Teilnehmer je einen persönlichen Schlüssel k_i besitzen, der nur dem betreffenden Teilnehmer und der Zentrale bekannt ist, **dadurch gekennzeichnet,**
   - daß in der Zentrale aus dem persönlichen Schlüssel jeder der n autorisierten Personen je ein Teilgeheimnis (Shadow) s_i abgeleitet wird,
   - daß in der Zentrale aus der Gesamtheit der so erhaltenen Shadows der autorisierten Personen ein (n,t)-Threshold-Verfahren (mit $t \geq 2n-1$) konstruiert wird,
   - daß in der Zentrale mit Hilfe dieses (n,t)-Threshold-Verfahrens aus den n Shadows $s_1, \ldots s_n$ ein Schlüssel k berechnet wird,
   - daß die Daten zur Konstruktion von k, die aus den zur Ableitung der Shadows s_i aus den persönlichen Schlüsseln k_i notwendigen Daten und aus $n-1$ weiteren Shadows des (n,t)-Threshold- Verfahrens, die sich von den Shadows der autorisierten Personen unterscheiden, bestehen, über den ungesicherten Kanal übertragen werden, und
   - daß autorisierte Personen empfangsseitig den Schlüssel k aus ihrem persönlichen Schlüssel k_i den ihnen zugeordneten Shadow s_i ableiten und aus diesem Shadow mit Hilfe der $n-1$ weiteren Shadows sowie dem (n,t)-Threshold-Verfahren den Schlüssel k berechnen.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß bei der Ableitung des Teilgeheimnis (Shadow) s_i in der Zentrale aus dem persönlichen Schlüssel für jede der n autorisierten Personen unter Verwendung eines gemeinsamen Parameters r und jeweils des persönlichen Schlüssels k_i unter Verwendung einer Einwegfunktion $f(\cdot,\cdot)$ das Teilgeheimnis (Shadow) in der Form von $s_i = f(r,k_i)$ abgeleitet wird.

3. Verfahren nach Anspruch 1 und 2, dadurch gekennzeichnet, daß das (n,t)-Threshold-Verfahren durch ein Polynom vom Grad $n-1$ realisiert wird, das durch n Stützstellen, zu deren Ableitung die Shadows verwendet werden, eindeutig definiert ist, und bei dem weitere Shadows dadurch gewonnen werden, daß die Zentrale Punkte auf dem Graphen des Polynoms auswählt, die von den aus den Shadows der autorisierten Teilnehmer gewonnenen Stützstellen verschieden sind.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß es zum sukzessiven etablieren einer Hierarchie von Schlüsseln verwendet wird.

– Leerseite –